Official Copy is	X Electronic	☐ Paper File

Defense Travel System

PKI Information & POC Listing

Version 2.0

Document Approval Page

The following organizations have approved this document as evidenced by signature and date contained herein.*

Signature _____ Date: _____

Col Larry J. Schaefer, Program Director, PMO-DTS

Signature _____ Date: _____

Weida Borkowski, Test & Integration Branch Chief, PMO-DTS

*Note: Original signatures are on file at the PMO-DTS

Document History

Control ID	Date	Version	Author	Description of Activity
PMO-GDE-T&I-112202-1.0	22 Nov 02	Preliminary	R. Mazur	Preliminary document routed for approval.
PMO-GDE-T&I-081204.2.0	8 Dec 04	2.0	R. Mazur	Change Kyberpass to Gradkell Systems, Inc.

TABLE OF CONTENTS

List of Figures

1 INTRODUCTION

The Defense Travel System (DTS) uses the DISA/NSA PKI system to digitaly sign a document. A digital signature will be used for authentication, data integrity and non-repudiation. Each traveler, or approving official must possess a valid Public Key Infrastructure (PKI) identification certificate. This guide is provided to the user community to help them understand the differences between software and hardware certificates, to document the different requirements of each, and to assist the site in providing their travelers the identity certificates they will utilize in gaining access to the DTS and for signing and approving travel documents.

1.1 Terms and Abbreviations

The following terms and abbreviations are used in this document:

ANSI	American National Standards Institute
AO	Authorizing Official
CM	Configuration Management
DFAS	Defense Finance and Accounting Service
DoD	Department of Defense
TDY	Temporary Duty
VPN	Virtual Private Network

Authorizing Official (AO). A supervisory official delegated authority to direct official travel, obligate travel funds in support of organizational mission needs, and approve travel claims.

Certification. The technical evaluation of a system's security features and other safeguards, made in support of the accreditation process, which establishes the extent that the particular system design and implementation meet a set of specified security requirements.

2 PKI COMPONENTS

2.1 Certificates

- Hardware – A certificate provided on a Common Access Card (CAC)
- Software – A certificate provided on a floppy (3 ½ inch diskette)

The hardware and software certificates issued by the DISA PKI interface are acceptable for use with DTS. The schedule for fielding CAC, which can be viewed at: www.dmdc.osd.mil/smartcard is issued and maintained by The Access Card Office of Defense Manpower Data Center East. While all sites are not on the schedule a site should be able to locate a CAC issuance office near them, or one that will be able to assist with their CAC

issuance. Once the deployment of CAC is completed the use of software tokens will be minimized. The use of software tokens will never be eliminated completely.

2.2 Public Key Enabling (PKE) Software

The PKE software utilized by DTS is a product developed by Gradkell Systems, Inc. This product is the only part of the PKI architecture that DTS retains control over. The user community is provided this software product with the license via download from the DTS website at www.defensetravel.osd.mil.

2.3 PKI Program Middleware Options

- Activecard Gold
- Spyrus
- Schlumberger
- Litronics
- Datakey

Middleware is a software product used to interpret PKI certificate information from either a CAC or diskette. It provides an interface with PK enabled systems, interprets files and provides certificate information to the PKE software (DBsign). The site/service will need to provide a middleware product from the list above for each workstation they have that will use PKE systems. DTS will interface with the same middleware products that other systems use but will provide DBsign as its PKE software. The products above are either in use or are included on the list of middleware products on the recently awarded enterprise license. For more information about the enterprise license you can visit the CAC ACO's web site www.dmdc.osd.mil/smartcard.

2.4 PKI Program Hardware Requirements

- Hardware Certificate (CAC)
    - CAC reader (w/ appropriate driver)
    - CAC
- Software Certificate
    - Diskette
    - Disk Drive

When a site deploys DTS and utilizes a Hardware Certificate they will need to insure that CAC's are issued and that each workstation has a CAC reader installed with the appropriate driver.

When a software certificate is issued, the site will need to insure an adequate number of diskettes are available and that each workstation has a disk drive capable of reading the diskettes. In addition, when fielding DTS with software certificates each site should be aware that in most cases a conversion to hardware certificates will be necessary in the future.

3 PKI FUNCTIONS

3.1 Software Certificate

As sites field Public Key Enabled systems like DTS they should be aware of the need to provide a level of PKI support. A service or DISA Registration Authority (RA) will appoint a Local Registration Authority (LRA) to issue site personnel software certificates. When fielding software certificates a site must appoint and train, at a minimum, one Local Registration Authority (LRA) to issue the certificates to their travelers and approving officials. Depending on the number of travelers a site may require more than one LRA and may appoint trusted agents to assist the LRA with the issuance of the certificates. Training for LRA's is documented in the Local Registration Authority Trainee Guide provided as part of the DISA LRA training. The site should contact their PKI POC listed later in this document, to coordinate with the Service Registration Authority (RA) to implement a PKI solution.

When an LRA or Trusted Agent has helped the user download his software certificates they will assist the user in exporting their certificates to a floppy disk. A very important part of this process is to identify the different certificates correctly to insure the user's Identity and Email Signing Certificates are properly labeled when they are exported to the diskette.

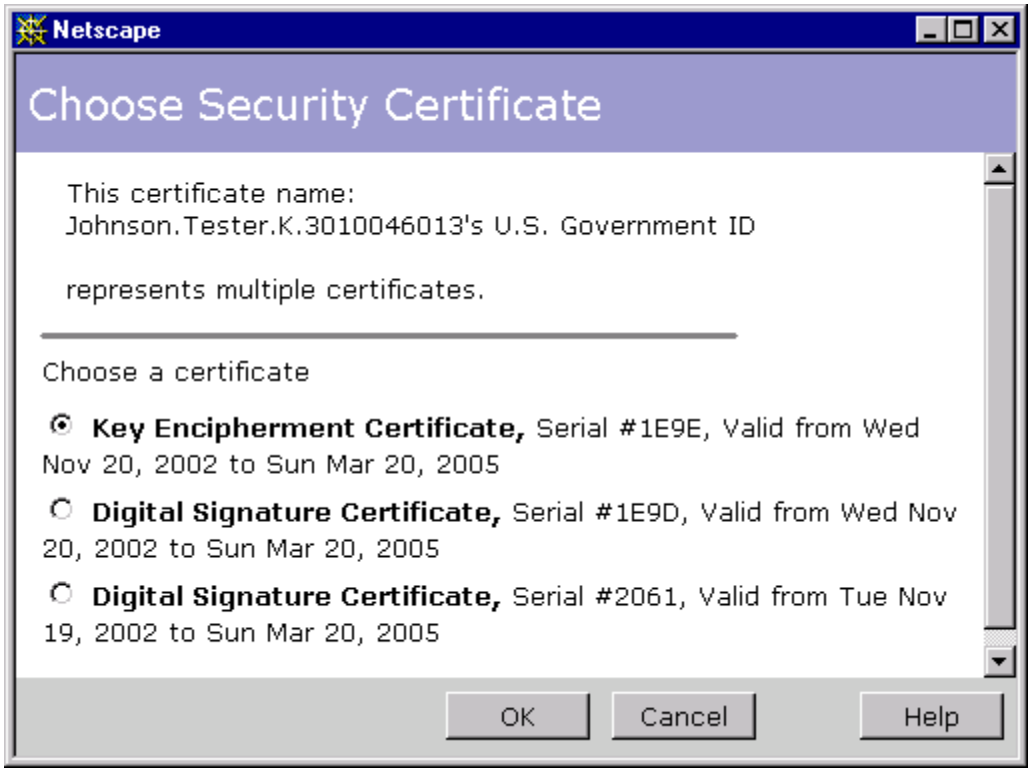

Figure 1. Security Certificate

If the LRA successfully downloads the Identity, Email signing, and Email encryption certificates for a user they will see the screen shown above. They are now ready to export the certificates to a diskette. The Encryption certificate is labeled Key Encipherment Certificate. The Email signing and the Identity certificates are both labeled as Digital Signature Certificates making them a bit more difficult to correctly identify. However, there is an easy way to distinguish between the two certificates when exporting them. If you will check the Serial # on the two certificates you will notice that one of the certificates labeled as a Digital Signature Certificate has a serial number very close to the number of the Encipherment Certificate (1E9D and 1E9E) and the other one's serial number is not anything like the Encipherment Certificate serial number (2061 and 1E9E). The Identity Certificate is the one with Serial # 2061 and the Email Signing Certificate is the one with Serial # 1E9D. When doing the export the LRA, or trusted agent, should save these certificates on the floppy making them easily identifiable as the identity or email signing certificates to the certificate owner.

3.2 Hardware Certificate

If sites field DTS and issue hardware certificates they can either deploy the hardware certificates from a mass issuance facility or via Verifying Officials (VO). The VO must have a RAPIDS workstation to interface with DEERS. The RAPIDS workstation will be updated under a separate fielding done by the Access Card Office of the Defense Manpower Data Center. The VO's will verify a person's identity, make sure they are in DEERS, and then issue them a CAC containing the Identity, Email Signing, and Email Encryption certificates. If a mass issuance facility is used to issue CAC's then the personnel in the facility will be VO's and perform the same functions.

4 POINTS OF CONTACT

4.1 Services

4.1.1 Army

Secure Electronic Transactions – Devices (SET-D)

https://setdweb.setd.army.mil

PMO-DTS Army IPT Lead

703-607-1498

4.1.2 Air Force

AF- PKI SPO San Antonio

https://afpki.lackland.af.mil

PMO-DTS Air Force IPT Lead

703-607-1498

4.1.3 Marine Corps

USMC MITNOC

DSN 278-5300

helpdesk@noc.usmc.mil

PMO-DTS Marine Corps IPT Lead

703-607-1498

4.1.4 Navy

Navy Information Assurance Website

https://infosec.navy.mil

PMO-DTS Navy IPT Lead

703-607-1498

4.2 Agencies

4.2.1 Defense Security Cooperation Agency

PMO-DTS Agency IPT Lead

703-607-1498

4.2.2 Defense Logistics Agency

PMO-DTS Agency IPT Lead

703-607-1498

4.2.3 PMO-DTS Agency IPT Lead

703-607-1498

4.2.4 Other PMO-DTS

PKI POC

703-607-1498